ARCHITIER

ARIES System Specification and Functional Requirements

Ike van Cruyningen, Quang Nguyen, Nick Wukich, Steve Solnit

December 29, 2003

1505 Black Mountain Road, Burlingame, CA 94010   650-343-7940   650-343-7950 fax

1 Executive Summary

The AIDS Regional Information and Evaluation System (ARIES) is a joint software project undertaken by four government jurisdictions: the State of California Office of AIDS, the County of San Bernardino, the County of San Diego, and the State of Texas, Texas Department of Health. The project is being managed by the Universitywide AIDS Research Program, a unit of the Office of the President of the University of California. The company selected to develop the software is Architier Corp.

While the Partners are developing the software jointly, they shall each run their own copy of the software, customized and configured for the particular business and legal requirements of their jurisdiction. To be able to host the software, each partner shall be required to set up and maintain a web server, a database server and a digital certificate server. To offload heavy system usage, each partner may opt to have a reporting database server where a copy of the data is stored just for reporting purposes. The Partner shall put the web server on the Internet, which would allow service providers to access ARIES by using the web browser on their desktop computers.

To use ARIES, providers shall need an account and password. To increase system confidentiality and security, all users shall also be required to register their computers with the Partner by obtaining a digital certificate, which authoritatively identifies the user each time he/she accesses the system. Additionally, all communications between the ARIES server and the user desktop shall be encrypted so that no other computers on the Internet could intercept the exchange and compromise client confidentiality.

The users of ARIES shall be able manage client records, run reports, import/export data and perform some administrative functions, depending on their permissions. This is done in a web-browser environment, which shall be designed to allow users to move quickly and easily through screens that have a consistent look and feel. With the client management functions, the user shall be able to:

- Enroll the client into the agency
- Capture demographic and medical information about the client, such as contact information, living situation, income, substance use, medical history, HIV and other medical tests
- Maintain and read notes and clinical assessments of the client
- Schedule the client for service at the agency
- Refer the client to another agency
- Define a set of action steps to help them achieve goals to improve their living, mental and health conditions
- Record every service provided to the client

System administrators of ARIES shall be able to configure and customize many of the features of the system through an administrator console. They shall be able to define who gets to access the system, what screen he/she sees and what actions the user can take on each screen. The System administrators shall also be able to get information about the system, such as the version numbers of all the software being used by the system and which users are connected to the system. They can log anyone out and prevent others from logging in.

The Partners and the program managers of the service providers shall be able to use ARIES to obtain detailed information regarding all services paid by private and public contracts and be able to break them into HRSA, as well as Partner- and agency-defined, service categories. Additionally, with most of the data in ARIES being kept historically, they can mine the data to determine such things as how often clients get CD4 tests and other indicators regarding the quality of care they receive.

2 Introduction

2.1 Subject and purpose of this document

After assuming the responsibilities for developing the ARIES system, Architier held a series of interviews with all of the Partners to determine what features and characteristics they wanted in ARIES. This document is the direct result of all those meetings. It details the functional requirements and system specification that the Partners collectively decided they wanted to have in the system. The document also provides a brief background on the project's participants and its objectives.

2.2 Intended audience and scope

This document is intended to define the features and characteristics included in ARIES. The Partners can use the document to remind themselves of the functionality they requested during subsequent phases of the project. The Architier software developers will get a broad understanding of the purpose and use of the software from the document and it will help them plan out an infrastructure that will be appropriate for the requirements contained within. To develop an actual application, the software developers shall rely on this document as well as a data element dictionary and a comprehensive set of screen sketches.

All the functionality and specification described in this document shall be incorporated in the final product, except for the items in Sec 7.1, and others where the context is clear that the item is an option that a Partner may choose for its installation, such as deploying a separate reporting server.

2.3 Organization of the document

This document is organized into four major sections: An introduction that includes a background on the project; a glossary of key technical terms used in the document; a description of the system specifications which spells out the general characteristics of ARIES; and a description of the specific functionality to be contained in the system. The functional specification highlights the capabilities and corresponding screen elements of ARIES, but a separate data element document shall officially specify all the data elements that shall be included in ARIES.

2.4 Project Background

2.4.1 Trends in HIV/AIDS Services

For more than ten years, Federal funding has been directed to local jurisdictions through the Ryan White CARE Act to help pay the costs of mounting an emergency response to the HIV epidemic. Working through states and Eligible Metropolitan Areas (EMA) administrative mechanisms, the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (DHHS) has been responsible for contract monitoring, interpretation of legislation, technical assistance, and progress reporting to Congress. (For additional background information, please consult the HRSA HIV/AIDS Bureau web site at http://hab.hrsa.gov; for a glossary of specific CARE Act terminology please see http://hab.hrsa.gov/history/webterms.htm).

Federal legislation has given preference to public health departments and mostly smaller nonprofit community-based organizations for the receipt of Federal funding to deliver HIV/AIDS services most appropriately at the community level. Especially in the case of EMAs, legislation also prescribes certain administrative responsibilities for local jurisdictions such as the establishment of planning councils that are responsible for conducting annual needs assessments, developing comprehensive service plans, prioritizing services, allocating funds, assessing consumer outcomes, and evaluating administrative mechanisms.

While HRSA contract compliance prescribes these duties, it has historically limited aggregate administrative expenditures for health system administration and health care management (including quality management) to 10% of total funding. In most cases, little or no funding has been applied to designing, developing, or operating effective and efficient management information systems to assist in planning, monitoring, or evaluating HIV/AIDS services. This is especially true in the case of grass-roots nonprofit organizations, which are traditionally predisposed to applying available funds directly to services for clients rather than to organizational capacity or infrastructure.

The design and development of management information systems utilized by HIV/AIDS service providers and health system administrators nationwide reflects an overall inclination toward meeting the minimum requirements of HRSA reporting. Providing effective tools for the planning, service monitoring, or consumer outcome evaluation functions that are understood to be essential to HIV service management or health system administration roles and responsibilities has been an afterthought.

After Congress reauthorized the CARE Act legislation in 1996, HRSA implemented more rigorous, accurate, and timely HIV/AIDS service delivery and outcome data reporting requirements. Several independent health system administration jurisdictions realized that their own management information needs were growing and that the ability to remain competitive for future funding would require more robust management information systems. It was in this environment that ARIES was conceived.

2.4.2 PARTICIPANTS

The AIRES project is a collaboration of four separate administrative jurisdictions: the State of California Office of AIDS, the County of San Bernardino, the County of San Diego and the State of Texas, Texas Department of Health. The goal of the partnership is to join together to design, develop, and implement an effective and efficient management information system meeting the current and future health care management and health system administration needs common to all four Partners.

The four Partners originally contracted with Nonprofit Management Solutions (NMS), a nonprofit management support organization, to investigate the Partners' respective current information management systems and to recommend alternative management information systems or initiate the design of a new system.

NMS produced a report based on site visits, document reviews, software and hardware demonstrations, interviews, focus groups and conversations with the Partners. The NMS report recommended that the ARIES Partners embark on the process of designing their own system.

The four partners contracted with the Universitywide AIDS Research Program (UARP) to define specifications for the new system called ARIES, which stands for AIDS Regional Information and Evaluation System. UARP's role is to manage the RFP for the software and to work with the selected vendor to produce the ARIES system. UARP was created by the California state legislature in 1983 in recognition of the need to take action in response to the AIDS epidemic. UARP is a component of the Special Research Programs (SRP) in the Office of Health Affairs, University of California, Office of the President.

Architier is the contractor that was selected to develop the ARIES system. The Architier team is responsible for meeting with all of the Partners to review the general requirements of the new system, which resulted in this document. Subsequent phases of the project involve:

- Developing paper-based storyboards for all the major screens in the application;
- Creating the data elements worksheet which documents all the data to be captured in the system and the options for fields where users are permitted to selected from a list;
- Producing a system design that divides work among the different tiers of the application, and documenting the decisions with UML diagrams;
- Creating the database, which includes the longitudinal database, the audit and error logs, as well as the main transactional database that stores information on clients, system configuration, and security. The logical structure of the database shall be documented in Entity Relationship (ER) diagrams;
- Designing the graphics, page layout and navigation so that the user has a consistent and pleasant interaction with ARIES throughout the entire application;
- Developing a pilot implementation that shall test one feature across all the tiers before starting full-scale development;

- Implementing the entire application;
- Testing and deploying the application;
- Producing training documents and training Partner system administrators and users (who shall be responsible for training the users from the service providers).

2.4.3 GOALS OF ARIES

The overarching goal of ARIES is to facilitate the delivery of effective, efficient, appropriate, timely, and desired services to people infected with HIV/AIDS. In order to accomplish this goal, the ARIES system must:

- Support the provision of HIV/AIDS services within the provider agency.
- Facilitate the coordination of health services between agencies.
- Use data captured in the process of providing services to:
  - Support program administration
  - Track services and payer source
  - Support program planning and evaluation

ARIES must be able to collect and report the information required by Federal and State granting agencies about clients and the services they receive. By the nature of the four separate jurisdictions collaborating on a single application, the system must be flexible and configurable to meet the individual requirements of each jurisdiction. Additionally, because some of the Partners are funded partially by another Partner, the system must also allow program data to be uploaded.

3 Terms and Definition

Below are key terms used within this document. Most deal with technology. The definitions are intended to provide a non-technical person with a general meaning of a term.

- **Application Server** – a software server that supports web browsers in using applications and databases that are managed by the server. This middle-tier server handles all the application operations, business logic, and connections for the web browser.
- **ARIES** – AIDS Regional Information and Evaluation System
- **ASP.NET –** Active Server Pages, a technology by Microsoft to create robust interactive applications for the Web
- **Certificate Server** – a server that permits a System Administrator to issue and revoke a digital certificate
- **Database Server** – a server that stores data in series of tables which contain columns and rows; secures access to the data; and controls what is added, updated or deleted from the tables based on user-defined rules
- **Digital Certificate** – an electronic identification card, issued by a certificate server, that establishes a user's credentials when doing business or other transactions on the Web
- **Encryption** – the process of disguising information in a way such that only the people with the right key can uncover the information
- **Entity Relationship Diagrams** – a diagramming methodology for describing the logical relationship between data elements of a database, regardless of how data is actually stored on the database server. The physical structure is dependent on considerations for performance and security.
- **Firewall** – a device or software that sits in front of a protected network and controls all data traffic coming from and going to the unprotected network, letting pass only data that meet certain rules defined by the system administrator
- **Gateway** – a system that joins two networks together
- **Historical –** in the context of the database, this refers to data that shall be kept in a segregated system that shall not be accessible by the ARIES application. Database triggers shall write old values to the historical database whenever a particular field is updated. The production system will maintain the one current value for the field.

- **HRSA** – Health Resources and Services Administration, a department of the US Federal Government whose stated mission is to direct programs that improve the Nation's health by expanding access to comprehensive, quality health care for all Americans.
- **HTML** – Hyper Text Markup Language, the standard language for describing how information is displayed and interacts with users on a web browser
- **HTTP** – a communication protocol that allows the web browser and web server to exchange data
- **HTTPS** – same as HTTP except it uses the SSL protocol to allow the web browser and the web server to agree to an encryption methodology so that only the two of them can decipher the communication sent to each other over the Internet
- **LAN** – Local Area Network, a self-contained collection of machines and servers that can connect with another LAN or the Internet via a firewall or gateway
- **Longitudinal** – this refers to data points that have multiple values over a period of time. Longitudinal data for certain data points shall be maintained and displayed in ARIES, until they are moved off the production database. At that point, they may exist only as part of the historical data. Examples of longitudinal data in ARIES are CD4, viral load, HIV tests, and pregnancy. Each client may have zero, one or more records for each other these fields.
- **ODBC** – Open Database Connectivity, a Windows standard that allows software to interact with a database by calling generic commands rather than specific and proprietary commands of any particular vendor's database.
- **OLE-DB** – the next generation of standards that encompasses ODBC and allow applications to work with data residing in emails, file directories and other non-relational forms, as well as the traditional relational database
- **Relational Database** – a type of database in which complex data is separated and stored across multiple tables, tied together by a common key, such as a Client ID. Doing this improves the flexibility of the database and increases its robustness.
- **SA** – System Administrator, a person responsible for configuring and running a system
- **SMTP** – Simple Mail Transfer Protocol, a protocol for sending/receiving mail over the Internet
- **SQL** – Structured Query Language, a standard language to create and manipulate data in a relational database
- **SQL Server** – a relational database server developed by Microsoft Corp

- **SSL** – Secured Socket Layer, a protocol that allows client/server applications to communicate in a way designed to prevent eavesdropping, tampering, or message forgery
- **Super-SA** – this account shall have permissions to configure and control every aspects of an ARIES installation, including assigning lower level system administrators.
- **TCP/IP –** a set of protocols that allow machines to communicate with each other and exchange data over a network
- **Three-tier architecture** – a methodology for developing robust and scalable software applications
- **UARP** – Universitywide AIDS Research Program, a component of the Special Research Programs of the Office of Health Affairs, University of California, Office of the President
- **UML –** Unified Modeling Language, a standard diagramming notation used by software developers to document systems, their users and actions
- **URL** – Uniform Resource Locator is the address of a web page
- **URN** – Unique Record Number, an identity number developed by HRSA that involves using a person's last name, first name, date of birth and gender
- **VB.NET** – Visual Basic, a programming language for ASP.NET and Windows
- **VPN –** Virtual Private Network is a private data network that uses the Internet as its telecommunication infrastructure, as opposed to other private networks that might lease a dedicated high-speed telecommunications line to link them. VPN uses a set of technologies to secure communication with all devices in the network
- **Web browser –** a desktop application, such as Internet Explorer, that processes the data exchanged with a web service, usually resulting in a display of a web page
- **Web server** – a server designed to process HTTP requests from a web browser, such as to get a certain web page or image
- **Windows** –the operating system developed by Microsoft for stand-alone laptop and desktop computers
- **Windows Server** – an operating system of Microsoft Corp designed to handle multiple user requests, such as in a web server or a database server
- **XML** – Extensible Markup Language is a cross-platform, software and hardware independent tool for transmitting information

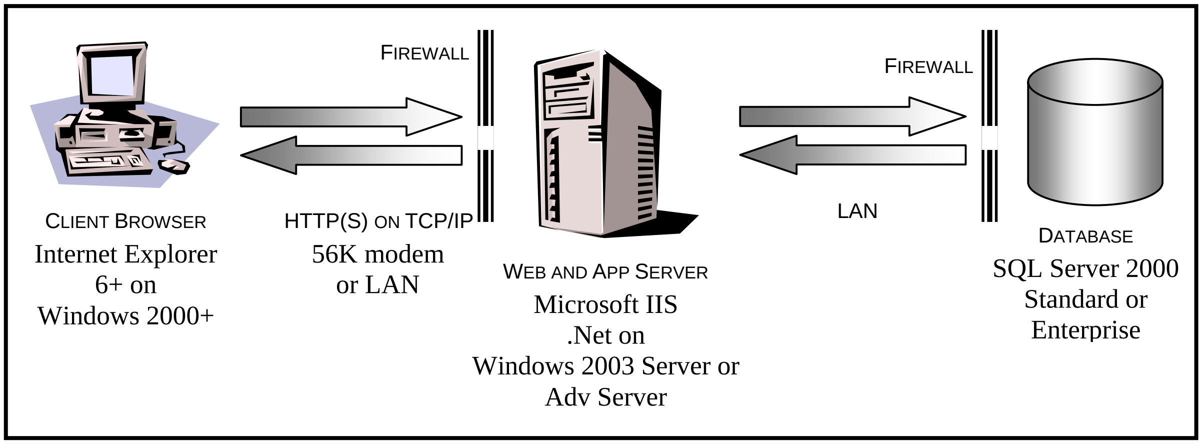
4 Project Overview

4.1 Project Goals

ARIES, the AIDS Regional Information and Evaluation System, is a browser-based client case management system that also fulfills administration and reporting needs for HIV/AIDS care. It will facilitate the delivery of effective, efficient, appropriate, timely, and desired services to people with AIDS and those infected with HIV.

4.2 System Technology

ARIES shall be a multi-tiered Web application with client, business logic, and data tiers running on separate machines. Each Partner shall host middle tier and database servers and their service providers shall access these servers through the Internet.



4.2.1 WEB CLIENT

The ARIES client application shall run inside Internet Explorer 6+ on Windows 2000+. It shall communicate with the middle tier through the Hyper-Text Transfer Protocol (HTTP) using Secure Sockets Layer (SSL) on a modem, cable, Digital Subscriber Line (DSL), or satellite connection.

When a case manager, receptionist, administrator, or other user enters the ARIES Uniform Resource Locator (URL) in their browser (Internet Explorer 6+), the middle tier shall return the Hyper Text Markup Language (HTML) for the login page. The user login, password, and a client-side certificate are uploaded to the application server to authenticate the user.

As the user works with the application, his/her requests and data entries shall be encoded in HTML forms. The HTML form input is validated with JavaScript in the browser and then transmitted over HTTP to the Web and application server. The middle tier processes these forms using data from the database. Then it produces HTML responses that are downloaded and rendered in the client.

4.2.2 Firewalls

To restrict unauthorized access to the servers from the Internet, the Partners shall install a firewall between their Internet connections and the middle tier server. This firewall shall limit communication to the HTTP and SSL ports. To further limit non-ARIES-based access to the database, Partners may opt to install a second firewall in front of the database server(s). ARIES shall be implemented using standard ports to ensure maximum compatibility with controls set on the firewalls (R97).

4.2.3 Web and Application Server

The middle tier is built on the Microsoft .Net platform. Internet Information Server (IIS) receives the HTTP requests and routes them to the .Net application server. ASP.Net pages are used to generate and process the HTML forms. The business logic is organized into separate VB.Net business objects using the Table Module pattern described in "Patterns of Enterprise Application Architecture", Martin Fowler et al. 1992.

4.2.4 Database

The client and service information, as well as much of the system configuration information, is stored in a Microsoft SQL Server database. A separate database on the same server is used to store the history of changes to the data as well as the transaction and security logs.

4.2.5 Reporting Server

Ad-hoc queries can place an unreasonable load on the operational database, so the Partners may opt to deploy a second database server solely for reporting. The operational data will be replicated to the reporting server periodically.

4.2.6 Certificate Server

All users of ARIES shall be required to have a valid account and password to access the system. As a second factor to authenticate the rights of the user to access ARIES, each Partner shall install a valid digital certificate on every machine that will access ARIES. A certificate server managed at each partner site shall issue all the digital certificates. The ARIES system shall reject any access to its resources by users or computers without a valid digital certificate.

4.3 System Functionality

The ARIES system has four major groups of functionality:

- managing client and service records (ARIES),
- administering system users and configurations (ARIESAdmin),
- moving data into the database (ARIESImport) and
- reporting on, and moving data out of the database (ARIESReportExport).

4.3.1 Client Management

ARIES will enhance services for clients with HIV by helping providers and Partners automate, plan, manage, and report on client data.

Client interactions start with a search of existing clients at that agency. If the client is found then a read-only screen displays tabs for all the major categories of client information. Within each tab are buttons to add or edit that category of client data.

Client Enrollment

If a client is new to an agency, the enrollment function starts with a check if the client has already been entered in ARIES by another agency. This search uses the components of the Unique Record Number. If the client is new to ARIES, then a series of screens collect eligibility, demographic, contact, income, insurance, medical, and risk factor data.

Needs Assessment, Care Plan, and Referrals

After the intake in system enrollment, a needs assessment screen displays a customizable initial needs questionnaire. For each identified need, a care plan entry with specific goals and tasks is developed. As part of the care plan entry, referrals can be made to outside services and appointments can be created for future visits.

Case Documentation

ARIES users document interactions with clients using

- Narrative case notes that are categorized by type of data
- Data fields for income, insurance, medical, outcome, and other discrete data
- Service line items for tracking work

Client and Service Reporting

Staff members at agencies use the reporting tools to create reports on clients registered at their agency and services rendered by their agency. These reporting tools include predefined, canned reports, as well as compliance reports, and a cross-tab wizard.

4.3.2 ARIES Administration

The system administration functions provide extensive access to the data and the system configuration tables. As a consequence, these functions shall be limited to a select group of users who possess a valid ARIES administrator client certificate. System management functions include adding and deactivating users and providers, adjusting user privileges and personalization, editing of lookup tables that populate the drop-down boxes, turning screen elements on and off for the different Partners, and viewing system configuration and logs. ARIESAdmin assumes advanced users who are intimately familiar with the system, so it packs a lot of functionality in the screens.

4.3.3 ARIES Data Reports, Imports, and Exports

Like system administration, ad-hoc data reporting, data import, and data export provide broad access to the database. Data for an individual agency shall be accessible from within ARIES via predefined "instant" reports and the cross-tab wizard. A more detailed ad-hoc report wizard, as well as bulk exports, shall be accessible in a separate ARIESReportExport application. The ARIESImport application shall support import of XML data into ARIES. To access ARIESReportExport or ARIESImport, the user must have a higher security client certificate. This provides better control and traceability for these applications.

The ad-hoc reporting in ARIESReportExport shall require a more sophisticated user who is familiar with database queries and the ARIES schema. For data import, the user is assumed to be extremely familiar with the external data system so they can format the data into the XML required for the ARIES import web services. For data export, the user must be proficient in the external data import functions of the destination application (Excel, Access, SAS, SPSS, and so forth).

4.4 System Users and Security Roles

Every user of ARIES shall be assigned to a role with the option of adding to or removing from the tasks associated with that particular role. There are additional qualifications to a specific task, such as an administrator only being able to create users within his/her agency.

The following is a list of the various roles in scope of the system, how the roles interact with ARIES and their impact on security and ability to perform operations (the exact default roles and their permissions/rights shall be established and documented further into the project development):

- Intake Personnel

  Typical activities performed include client enrollment, finding existing records in the system, updating client information, scheduling appointments and referrals, and recording client encounters. These users shall access the application only from the ARIES client.

- Case Managers (medical and psychosocial)

  Typical activities performed include recording case notes, recording client assessments, service eligibility verification, scheduling appointments and referrals, case conferencing, recording client encounters, determining client acuity, developing individualized service plans, entering treatment plans, and monitoring the implementation of these plans. These users shall access the application only from the ARIES client.

- Clinicians

  Typical activities performed include treatment of patients (physical health, mental health, etc.), entering treatment plans, and reviewing and approving treatment plans entered by Case Managers. These users shall access the application only from the ARIES client.

- Provider Agency Managers

  Typical activities performed include comparison of productivity, budgeting, tracking of services, tracking of payer source, modifying staffing patterns, demographic reporting, and tracking treatment for the purposes of program planning and grant writing. These users shall access the application from the ARIES and ARIESData clients and can impact the database performance with large queries resulting from their reporting and exporting activities.

- Support Services Providers

  This category includes food services, transportation services, ancillary quality of life services, etc. Typical activities performed include the documentation of encounters and services rendered, and ongoing tracking of provided services. These users shall access the application only from the ARIES client.

- Data Users

  This category includes public health administrators, epidemiologists, health planners, health researchers, analysts, and other users who need the ARIES system for reporting purposes or need to extract data from the ARIES system for client level and aggregate reporting, for planning, for program evaluation and for other analysis. These users shall access data from both the ARIES application, the ARIESReport/Export application, and (optionally) with direct connection to the database via ODBC or OLEDB. If their reporting and exporting activities degrade database performance, then the Partners may opt to set up a separate reporting server.

- ARIES Provider System Administrators

Typical activities performed include managing user accounts for their agency as well as any other system administrative tasks delegated to the agencies. These users shall access data from the ARIES client.

- ARIES Partner System Administrators (including Super-SA)

  Typical activities performed include configuration and maintenance of the ARIES system. These users shall have access to all components of the system.

5 System Specification

5.1 Architecture

The ARIES system incorporates four different Web applications,

- ARIES for operational users who typically work with one client at a time (Intake Personnel, Case Managers, Clinicians, and Support Services Providers),
- ARIESAdmin for Super System Administrators,
- ARIESReportExport for data reporting and export, and
- ARIESImport for data import.

This separation both simplifies the individual applications and enhances security. Simplifying the individual applications makes it easier to provide user interfaces that are intuitive (R80) and well organized (R81) for each specific role (R2). This reduces training costs and encourages correct usage of the application.

The different applications have significantly different security versus accessibility requirements. ARIES operational users access small parts of the database from almost any Web browser. ARIESAdmin users access critical configuration and security tables from a limited number of machines within the firewall. ARIESReportExport users have access to more data from a restricted set of client machines. ARIESImport users can upload new or updated information into the database.

The four applications all run on the same middle tier server, share the same database, and are built on the same infrastructure.

5.1.1 Three Tiers

The web applications (R83) use a standard three-tier architecture (R84) built with Microsoft development tools and technology (R83). The three layers and their roles are:

- Presentation – handles the display of information and the interaction between the user and the software.
- Business Logic – interprets the commands from the users that were received through the web browser, for example, creating a new record, and applies

whatever rules might be appropriate, such as requiring that a particular eligibility document be present.

- Data – communicates with the systems that store or process information such as a database

The Presentation layer shall run within Internet Explorer 6+ at an agency site. The typical physical set up at a Partner site shall be a web/application server with HTTP and HTTPS ports exposed in the external firewall. The relational database server shall be a separate machine residing in the private network and shall not be accessible over the public network (R65).

5.1.2 Real Time Performance

The ARIES system shall process records (add, update, and delete) in real time (R3). Whenever a Save or Apply button is chosen on a form, any data that has been entered into the form shall be validated and sent to the middle tier, checked against the business rules, and stored in the database. All this processing shall occur within a few seconds. There shall not be any deferred updates (such as entering a service line item today but not having it recorded in production until another date in the future), queuing for delayed processing, or any store and forward capability.

It is difficult to predict latency and throughput in Internet connections (particularly for large downloads like lists of medications), so performance shall be tested on a LAN with computers that have caches loaded. When tested in a LAN with a warmed-up cache, every screen in ARIES shall display in three seconds, plus another second per hundred rows of data. Report output, data export, and data import can take longer, depending on the complexity of the report or data transfer.

In situations where the system is not accessible (e.g. crisis situation, in-home or off-site visit, case manager uncomfortable with data entry during an interview, network down, or system down), users shall record data on paper for later data entry.

5.1.3 Scalability and Availability

ARIES shall support at least 800 concurrent users performing normal system operations (R99). Extensive ad-hoc reporting (R100) can place an unreasonable load on the database server, thereby slowing system response. In this case the Partner must install a separate reporting server to handle the load.

The server hardware and software for ARIES shall be standard, commercial quality to ensure good uptime characteristics (R101). If a Partner requires guarantees for uptime, then they may opt to purchase redundant machines, fail-over or load-balancing switches, and parallel database software.

5.1.4 Localization

To support future localization (R9), the screen HTML with the titles, labels, button names, etc. shall be separated from the business logic using the .Net code-behind structure. Localization for a new language shall require changes to the HTML, but not to the application logic. Combo boxes and other screens elements listing descriptive values shall be filled from database tables containing these descriptive or configuration values. Localization of these values shall require a parallel set of values for the new language. Error messages shall be stored in a separate application-level XML file with branches for each language. Localization of these messages for a new language shall require a new branch in the XML.

5.2 Web Clients

To access ARIES, users enter a URL in their browser (R83), Internet Explorer 6+ (R95) on Windows 2000+ (R94). There shall be four URL's for each Partner to access the four components of the system: the client management, data import, data report/export and the administrator console. For Partners who will distribute digital certificates over the Internet, there shall be one more URL for the digital certificate server. Each ARIES URL retrieves an HTML page to collect the login and password.

To support strong two-factor user authentication (R62, R63), each ARIES client must also have a digital certificate installed as part of the client setup. The user (or a technical support staff) shall need to install the certificate, using the instructions provided by the Partner, on each of the computers where the user will access ARIES. The installation will occur whenever the user is issued a new digital certificate, including the time when an old one has expired.

When a user starts to use ARIES, the login, password, and certificate credentials are transmitted over HTTPS/SSL (R1, R67) to the server. Based on the user's role, different screens and different elements in screens in the application shall be visible and accessible (R1, R70, R71). ARIES shall operate over a modem connection for individual client records but for reporting and a better user experience, a faster connection is recommended. (R96)

5.2.1 User Interface

Users download HTML pages containing forms to work with the application in wizard-style sequences. These sequences correspond to the typical workflows for these users to ensure they find the system intuitive, easy to use, and easy to navigate (R2, R80). Client data shall be grouped into tabs and the corresponding edit screens to match the service provider's view of the system (R81) with a consistency in layout, use of controls and color (R82).

Standardizing on IE 6+ and avoiding frames makes it easy to provide a good keyboard interface (R2). Keyboard shortcuts shall include 1) Enter and Cancel for each form, 2) access keys or mnemonics (Alt + underlined letter) to quickly jump to a specific control within one form, and 3) accelerators (Ctrl + letter) valid in all pages to perform a specific function (e.g. text cut, copy, paste) or jump to a specific screen. ARIES shall provide a combo-box type-ahead feature so that users can easily make their selections in long lists.

5.3 Web and Application Server

The middle tier for generating the HTML screens and implementing the business logic shall use Microsoft .Net (R85, R86) running on Windows 2003 Server or Advanced Server (R87). The Web server, Internet Information Server 5.0 or 6.0 (R91), is tightly integrated with .Net.

The individual screens shall be built from HTML templates to promote consistency in layout, use of controls, and use of color (R82). Using the ASP.Net code-behind approach separates the screen layout from the form processing, making it easier to customize the layout for different partners (R6, R17, R31) or to support additional languages (R9).

Business logic shall be organized in separate, extensible components (R7, R8) using the Table Module pattern described in “Patterns of Enterprise Application Architecture”, Martin Fowler et al 2002. The middle tier shall use VB.Net.

The minimum hardware specification for the middle tier servers is:

- Pentium Xeon 3.06GHz
- 512 MB RAM
- 36GB Hard Disk
- 100 Mbps network connection

The web and application server shall also be compatible with the following applications running on the server (R93):

- Diskeeper
- Trend Antivirus
- Symantec Antivirus
- BMC Patrol Agent
- Veritas Backup Exec

5.3.1 Error Handling

Error handling shall be through the .Net validation controls and .Net exception handling mechanisms with English language error messages (R5). Whenever possible the error messages shall be displayed in red at the top of the form where the error occurred. For broader scope errors (e.g. session timeout or database connection lost) a special error page shall be displayed. Application error logs shall be tab-delimited text files containing date, time, user ID, screen name, parameters, error code, error message, and the program stack at the time of the error. These files can be imported into Excel or other analysis tools, if desired by the user. Depending on the configuration of the partner installation, the error log may be stored in the Windows application event logs instead of a text file.

5.3.2 Database Access

Database access from the middle tier shall be through the .Net interfaces that are compatible with the version of Crystal Reports built into .Net as well as Crystal Enterprise (R98).

5.4 Database

The database shall be SQL Server, either Standard or Enterprise edition (R88) running on Windows 2003 Server or Advanced Server (R87). Architier shall provide the hardware guidelines when the requirements have been signed off and the database designed (R92). The database can be placed behind a second firewall to control access (R65). SQL Server supports ODBC and OLE-DB interfaces for querying tools (R98).

The database schema shall be developed after the screen sketches are complete, and it shall employ constraints to ensure quality of the data, foreign key relationships to ensure referential integrity, and indexes for performance (R89). The columns containing sensitive, identifying data shall be encrypted (R64).

The minimum hardware specifications for the database server(s) are:

- Pentium Xeon 3.06GHz
- 1 GB RAM
- 72GB Hard Disk

For optimal performance and/or recovery, the Partners may consider SCSI drives, RAID and dual processors.

5.4.1 Data History and Audit Trail

Changes of client information in the primary database shall trigger an insert of the 'before' data records in a separate logging database (R10). This provides an audit trail of changes (R68). The historical table shall contain all the columns of the original table plus the datetime of the change and the userID making the change. Storing historical data in a separate database keeps the operational database small and simplifies discarding of old data. It does make reporting on historical data more difficult.

Once a record is created in ARIES, be it a client, user, provider or service record, it cannot be deleted using the front-end. Users shall be able to change the status of records from active to inactive (in addition to others as appropriate). The system shall have the ability to let qualified users deactivate or disregard a record (R32), which shall prevent the record from being viewed again, such as in the case of creating a duplicate record.

5.5 Customization

While the Partners agree on core functionality, each will require customization of the implementation for certain features. This customization shall include

- Setting system configuration options such as authentication timeouts (R6)
- Changing the entries in drop-down comboboxes (R44)
- Hiding or displaying data entry fields on screens
- Adding custom fields to the ends of screens (R17, R19, R26, R31, R37)
- Customizing the service hierarchy to reflect different programs and service categories (R22).

For more extensive customization of the business logic or security rules, the Partners are able to enhance the application with Visual Studio, an excellent development platform. Further changes in screen layouts are easily handled since the HTML is separated from the forms processing through the .Net code-behind approach. With access to full source code, there are no limits on future customization and enhancements.

5.5.1 System Configuration Options

System configuration parameters such as authentication timeouts, display limits on search results, and login retries shall be stored as name-value pairs in a standard web.config file. ARIESAdmin shall include a screen to edit the values in this file. When using the administrator console to manage the configuration file, the Super-SA shall have the option to encrypt the value of a key. Doing this shall prevent any sensitive information from being stored in clear-text in the configuration file. The storage location of the database login and password shall be determined during the database design phase.

5.5.2 Drop-down List Customization

The drop-down lists in the data entry screens shall be customizable through a screen in ARIESAdmin. When the Super-SA user chooses the data entry screen name and the drop-down list name, he or she shall be able to define the display text, data value, display order, and visibility of every entry in the list.

5.5.3 CONTROLLING VISIBILITY OF DATA ENTRY FIELDS

Partners can hide individual data entry fields through a screen in ARIESAdmin. When they choose the data entry screen name, the screen shall display a list of available fields. They shall then choose to hide any of these fields, or to redisplay fields that have been previously hidden.

5.5.4 ADDING CUSTOM DATA ENTRY FIELDS

To support the customization with additional data elements, the database shall have two tables to store customization options. The tables and their respective columns are:

CustomData:

- ClientID
- CustomElementID (References CustomElements)
- DataValue
- DateEntered
- UserID

CustomElements:

- CustomElementID
- ElementType (string, integer, date, and other .Net types)
- Purpose (Enrollment (R17), Intake (R19), Service (R31), Quality (R37))
- DisplayScreen (aspx filename where input field will appear)
- DisplayOrder
- RequiredField
- ValidationControl (.Net controls)
- ValidationExpression (depends on validation control)
- ErrorMessage

This approach supports flexible addition of data elements at the Partner level. For data input, the additional labels and text entry fields from the CustomElement table are appended to the bottom of the screen in DisplayOrder. The values the user enters are checked on the client and/or in the middle tier. When the user submits the form, the middle tier inserts or updates the values in the CustomData table. For reporting in a data export, the user determines the CustomElementID from the CustomElement table and then extracts the values from the CustomData table.

Custom data fields shall use the same historical tracking as other fields. Security shall not be supported at custom element level, except in so far as the entire data entry screen is available to that particular user.

5.5.5 Custom Service Hierarchy

ARIES includes a four-level hierarchy of programs and services that controls the entry of service line items. The first three levels are customizable by the Partner, while the fourth level is customized for the agency during agency setup. Partners shall configure an XML file, ServiceHierarchy.xml, to reflect the program and service hierarchy suitable for their deployment. This file shall include the names and abbreviations for each program, service, and subservice. The subservices shall also include links to CADR categories for reporting, default units, default quantities, and default costs for units of service.

5.6 Security

In collecting the requirements for the ARIES system, Architier elicited detailed security and confidentiality requirements from each Partner (R61). All of the requirements that were agreed upon have been addressed throughout this document, in addition to the requirements specified in Attachment H of the original RFP (R79). This section discusses some of the general security characteristics of ARIES, both built-in and incorporated from third-party sources, which shall exist to ensure client anonymity, privacy and confidentiality.

5.6.1 Internet Communication

All communication between the client and the application server shall be encrypted using the secure sockets layer (SSL) (R67). This ensures that no one shall be able to tamper with, or eavesdrop on, the network packets. It does require more processor power on both ends of the communication to encode and decode the messages.

Communication between the application server and the database server(s) shall be on a LAN behind a firewall. We shall recommend a non-standard port for the database communication.

5.6.2 Firewalls

The Partners shall install a commercial firewall in front of the application server to prevent unauthorized access. They shall configure the firewall to limit communication to HTTP and HTTPS with the agency IP addresses.

To further limit non-ARIES-based access to the database (R65), Partners may opt to install a second firewall in front of the database server(s). This firewall shall prevent all access other than the database communication on an unusual port from the IP address of the application server.

Architier shall provide a list of commercial intrusion detection tools with the installation and setup documentation (R69).

5.6.3 Encryption

Communication between the browser and the application server will use SSL so it is encrypted. Likewise communication between the application server and the database may be configured to use SSL for encryption. The ARIES system shall provide the option to encrypt data in the database (R64, R52, R59); and this data shall be encrypted and decrypted on the database server.

5.6.4 Authentication

ARIES shall require two-factor authentication with a user login and password, as well as a client certificate, to access the applications (R62, R63). Two-factor authentication is based on something a user knows (factor one, the login and password) plus something the user has (factor two, the digital certificate). In order to access a network, the user must have both factors, just as he/she must have an ATM card and personal identification number (PIN) to retrieve money from a bank account. This provides a much more reliable level of user authentication than reusable password. This probably shall require incorporating a third-party product for the authenticator.

Each user shall be assigned a login and a password. The Partners shall have several configuration options for managing passwords:

- The password expiration in days allows a Partner to enforce password aging. Users shall be requested to change their passwords when the password expires.
- The password regular expression defines the signature for a valid password.
- The limit on password attempts records repeated failures and then locks the account.
- The lock time in minutes allows a Partner to adjust the time the account is locked (or use 0 for a permanent lock).

Every user must possess a valid digital certificate to access ARIES. Each Partner shall install Microsoft Certificate Server to issue all the digital certificates for that deployment. The ARIES system shall reject any access to its resources by users or computers without a valid digital certificate. The system shall support four levels of certificates for access to ARIES, ARIESImport, ARIESReportExport, and ARIESAdmin.

5.6.5 Authorization

Besides requiring an account/password and a valid digital signature to access ARIES, the system shall have other controls in place to secure data and protect confidentiality. Each major functionality grouping (Case Notes, Care Plan, Demographics, etc) shall be controlled to restrict a user from viewing, adding or editing data (no one shall be able to delete records). To view, add, or edit data in a particular functionality, the user must have permissions to view, add, or edit the data, as defined in his/her account setup. The ARIES system shall restrict the viewing of data by unauthorized users by not displaying links to the data or any other hint that the data exists. To restrict adds and edits, the system shall not display the add or edit buttons for users not granted those permissions.

To control what parts of a client's record a user gets to see, the System Administrator shall assign them to the appropriate security role. (Each partner shall determine whether the providers shall be able to manage accounts for their users, so the term System Administrator in this context refers to anyone processing the privileges to manage user accounts and permissions.) Each role shall be predefined with a set of permissions to view, add or edit data within a particular functionality. The SA shall be able to grant a user permissions above what is defined for the role, as well as deny the user any permission granted to the role.

Some controls shall be built directly into the system, such as limiting the view of mental health, substance abuse, and legal notes to only the agency where the note was created. While the Super-SA shall be able to configure if such restrictions apply at an installation, once a hard-code control is opted, changing a user's security role shall not circumvent the control.

Another example of security controls built directly into the system pertains to managing client record sharing. Clients shall have the right to agree to share or not share their data with all providers within a Partner installation (R77). Once a client has agreed to share, he/she shall be able to grant a provider access to his/her record only by providing the agency with all of the components of the client's extended Unique Record Number (R73, R74). Without the URN, the agency would have to create a new client record. Once a record is shared, a provider shall be able to see all appropriate parts of the record, as defined by the functional requirements. An agency shall never be able to report on service records, or things of the similar strain, that were not created by the agency.

5.6.6 Security Log

The SQL Server transaction log will log all changes to the database (R68). Furthermore changes to the data shall be tracked in the historical database (see Section 5.4.1).

Additionally ARIES shall track the details of all login attempts (date, time, login, client certificate, and whether successful or not). The Super System Administrator shall be able to configure the system to output log information to a delimited text file or the Windows application event log (R47).

5.6.7 HIPAA

The different Partners interpret the HIPAA regulations quite differently. To ensure compliance with any interpretation of the HIPAA regulations, ARIES shall provide a Partner configuration option to turn off all sharing of client data (R70).

5.6.8 Administrative Agencies

If an agency is granted permission to create other agencies, then it becomes an administrative or lead agency. The administrative agency manages all the agencies it creates and is allowed to see all their data. The Partner may change the agencies managed with a separate screen in ARIESAdmin.

6 Functional Requirements

6.1 Client Management Functions

6.1.1 System Enrollment

With the System Enrollment function, users shall be able to add new clients to the ARIES system (R11). To minimize the potential for adding duplicate clients (R4), the user must first attempt to find the client through both the agency-specific and ARIES system-wide search screens (R13). If the client is an existing client of the agency, the user shall be able to locate the record quickly by entering partial identifying data, such as the client’s last name or agency client identifier, into the search screen. If no record is found, the user shall need to do an exact system-wide search using the components of the extended Unique Record Number (eURN). If no match is made with the eURN, then the user shall be presented with the ability to create a new client record using the New Enrollment functions. These capture the data needed to generate the URN, the eligibility documentation, and then continue with the Intake functions.

To uniquely define clients, HRSA has created an algorithm to generate a URN (see CAREWare documentation at http://hab.hrsa.gov/careware/). This URN is based on the client’s last name, first name, date of birth and gender (using the HRSA options for male, female, transgender and unknown). This algorithm does not always produce unique values, so it is being extended by HRSA with an additional letter to discriminate duplicates. This approach does not work in a shared environment so ARIES shall work with an extended URN based on the original HRSA fields plus the client's middle initial and the first and third characters of the mother's maiden name (R12). In compliance reports and exports, ARIES shall support the HRSA URN definitions.

Once the URN’s are created, the system shall collect a small set of data to complete the New Enrollment (R14). The specific elements collected at this stage shall be configurable for the Partner installation (R17). The elements that shall be configured in the default installation include:

- Eligibility Documents such as HIV Diagnosis, Income Statement, Residency Statement and Consent Forms (R19).
- Referral Source which shall be a pick list of either generic categories or specific providers, depending on the configuration for the Partner installation (R15)
- Intake/Enrollment date (R16), which shall not be editable once saved, except by a high-level system administrator under clearly defined policies and procedures. The initial value for this field shall be blank to ensure that the user consciously enters an appropriate value.

ARIES shall allow users to manage the client’s various eligibility documents, such as Income Statement, HIV Diagnosis, Consent Forms and Residency Statement (R19). For each document, the system shall keep information on the document date, when the user received it, its source, where it is kept, and notes. The list of eligibility documents displayed shall be customizable by the Partner.

6.1.2 INTAKE

Once the New Enrollment is completed for a client, the user can capture the balance of the client’s demographic and medical information using the Intake functions (R18). This function captures data such as the client’s contact information, living situation, ethnicity, languages, education level, income, health care, medical and mental health history, as well as risk factors. Income information entered for the client shall result in the Federal Poverty Level being calculated and displayed on screen. The Data Element Document being developed for the ARIES project details the entire dataset for the Intake.

Because information about a client is so broad and diverse, the system shall organize a client’s records using a tab interface, which allows a large amount of data to be grouped and displayed in small chunks. There are nine tabs: Demographics, Eligibility, Programs, Medical, Medication, Risk Factors, Care Plan, Case Notes and Services. During the intake process, the user shall go through a series of screens that will complete out the information on each of these tabs, discussed in some detail below. (The screens will not correspond one-to-one to a tab, since a tab will contain data from a number of screens.)

Contact Information: This is the client’s current and previous address, in addition to the mailing address and the emergency contact. Each address shall allow the user to enter the street lines, city, state, ZIP Code, county and Geographic Area. The user shall be able to specify if mail can be sent to the client, and whether communication with the client shall be kept discreet. On this screen, a user can enter several telephone numbers where the client can be contacted (work, home, mobile, fax, and so forth). The user can specify for each phone number whether the client can be contacted at that number, if the user needs to be discreet and whether he/she can leave a message.

Living Situation: In this screen, the user shall enter information about the client's current and previous living situations. The user can provide information on the type of housing assistance the client has, as well as some data specific to the HOPWA housing program, such as gross adjusted income and the number of bedrooms in the unit.

Basic Demographics: This screen shall collect race/ethnicity, which languages the client uses to speak, write, and read, as well as information on the client's sexual orientation, marital status, veteran status, educational level and special needs for physical disabilities. The user can also enter an alias for the client and his/her social security number.

Financial: In this screen, the user shall be able to provide detailed information about the sources of income that a client has, from employment/wages and insurance through a number of public income such as SSI, SSDI and Food Stamps. The user can specify if the income figures provided are calculated based on monthly or annual amounts. Besides the individual income, the user can specify household and family incomes, with the number of people in the household or family. When these values are supplied, the system shall automatically calculate the client's Federal Poverty Level.

Insurance: This screen captures the client's private and public health insurance coverage. For each source of insurance, the user shall be able to specify the type of insurance; if coverage is pending; if the source is primary and pays for most of the client's medical bills; the carrier; the policy number; the start and end dates of the insurance; the monthly premium and any note about the source of insurance. If the client has no insurance, the user shall click on a checkbox specifying that.

Basic Medical: The Basic Medical screen is a series of sections dealing with medical care, the client's HIV tests and details about his/her AIDS status, where appropriate, as well as information about weight, allergies and assessment scales. The system shall permit the user to indicate where the client gets his/her general and HIV medical care, and the primary providers for each. In the HIV testing section, the system shall allow the user to capture each HIV test that the client has taken, record the results and provide information about pre- and post-test counseling that the client might have received, and indicate if sexual partners had been notified. The AIDS Diagnosis section details the date AIDS was diagnosed and the various defining conditions such as Toxoplasmosis, Pneumocystis Carinii Pneumonia and Cytomegalovirus. As part of the medical data, the system shall include the ability for users to record answers to a Karnofsky or Cognitive and Functional Ability Scale assessment. Partners have additional acuity tools that differ in their format and questions. To support these acuity tools, ARIES shall provide links to external Web pages that present the appropriate instructions and questions for establishing the client's particular acuity score. The user shall transfer up to four numeric or textual values that would be stored as part of the client's acuity assessment in ARIES.

Medical History: This screen captures information on the results of the client's medical tests, including: CD4, Viral Load, STI/Hepatitis, TB and immunizations. With the STI/Hepatitis and TB data, the system shall allow the user to indicate if the user sought and obtained treatment for the condition.

Information Specific to Female Clients: This section shall appear only for female clients. It allows the user to enter information about the client's primary OB/GYN medical provider and input pap smears/pelvic examinations. The screen shall also provide the ability to capture information regarding the client's pregnancies and transmission of HIV to the infant.

Medications: In this screen, the user shall be able to enter medications prescribed to the client, both anti-retroviral therapies (ART) and others types of medications. The system shall capture the names of the prescribing doctor, the pharmacies, and the start and end dates and the dosage of the prescriptions. The user shall be able to record basic questions about the client's adherence to his/her ART medications.

Risk Factors: This screen details the risk factors for the client's HIV exposure. It shall also provide the ability to capture information regarding the client's mental health and substance use history.

Once the client has had the initial intake completed, the system shall allow the client to be assigned a Case Manager (R27) and other staff. This assignment may be on a program-by-program basis or in a separate staff assignment screen. The staff member's name, agency, telephone number, and other details are stored in the staff profile.

6.1.3 Needs Assessment, Care Plan, and Referrals

The ARIES system shall include a function that shall allow a caseworker to perform initial and recurring assessments of a client's physical, mental, psychosocial and personal needs (R21). The assessment begins with a screen listing Partner-customizable needs categories (R22). For each indicated need, the user shall elect to create an entry in the Care Plan. The needs questions shall be tied to the service hierarchy to prefill many of the entries in the Care Plan.

In a care plan entry, the user shall define the need that is to be addressed for the client and the goal desired. Each care plan entry shall have a number of associated tasks and referrals for the client designed to achieve the stated goal. Each task shall be assigned to the client or a staff member (or referred to an outside agency) to complete by a target date. At some point in the future, the staff member assigned to the task or the user who had created the care plan shall update the task to indicate if that task was completed, in progress of being completed or some other status. The person editing an outcome shall be able to set a date the outcome occurred and include a brief note. Besides the outcome of the individual tasks, the care plan itself shall have a field in which a user can specify the status of the overall plan.

The care plan shall be designed to allow the user to create an individualized service plan for the client, who at the end of the meeting with the staff shall get a printed copy of the plan to sign to indicate his/her agreement with the course of actions (R26). The categories of the care plan match the service hierarchy. Users shall be able also to specify "Other" if none of the categories/subcategories meet their requirements. In that case, they shall be required to complete a textbox detailing what the "Other" is.

A care plan might entail a referral to another service provider, either internal or external to the user’s agency (R23, R24). When making a referral, the user shall specify the service categories for which the referral is being made, and the target and follow-up dates and reason for the referral. The client, at his/her choosing, shall initiate contact with the referred staff/agency. The system shall not have any active mechanism to initiate a referral. For external referrals, the client must provide all the necessary components of his/her extended URN at the other agency to permit access to his/her records (R73, R74). After accessing the client’s records, the referred staff/agency shall be able to pull up the referral, complete an outcome for the referral and indicate if the service requested was provided to the client, in addition to recording any notes about the service.

6.1.4 Case Documentation

The ARIES system shall provide a function to document all encounters with a client and capture narrative information (R25, R28, R30). This shall be done using a notes screen for all disciplines.

The user begins by entering a staff person and the date of the activity. Then they choose a type of note, whether it is an Intake, Progress, Reassessment, Crisis, Group, or Case Conference note. This assists in retrieving specific types of notes in reports.

Then the user enters sections or paragraphs of narrative, choosing a category for each one. The categories include Presenting problem, Medical, Financial, Housing, etc. These categories serve to restrict the visibility of the note to other agencies. Legal, Mental Health, and Substance Abuse notes are never shared. Other categories may be shared, but the user always has the option of checking a "Don't share" checkbox to prevent other agencies from seeing that note.

Progress notes shall be editable by the creator until they are signed and sealed by the user. The system shall allow a supervisor to countersign a note entered by a user, such as in a situation of clinical interns. An unsigned note shall not be viewable by another agency. Once a note is signed and sealed, it shall become viewable by another agency, if that is appropriate for the note category and its privacy setting. After the note is signed and sealed, it shall not be editable except by higher-level users under specific policies.

6.1.5 Scheduling Appointments

ARIES shall include a scheduling calendar that allows the user to make an appointment for a prospective or a client to receive services at the agency (R20). The calendar shall track:

- The potential client's name
- Date of birth
- Telephone number (if there is one)
- Their language requirement
- Date and time of the appointment
- Source of referral
- Staff person whom the client is scheduled to see
- The scheduler's name and telephone number
- The reason for the appointment
- Whether the agency needs to be anonymous when contacting the client for an appointment reminder.
- The childcare or other special needs of the client
- The outcome of the appointment (whether it was kept, rescheduled and so forth)

6.1.6 Quality Management Functions

These types of functions help program managers ask questions about the quality of care clients receive, such as how many clients are getting quarterly CD4 tests. Most of these types of information shall be derived from reports within the system, using data kept longitudinally (R35). Below is a list of information that shall be tracked by ARIES to support the standard quality indicators featured in HIVQual (R36):

- HIV Staging (viral load, CD4 count)
- Antiretroviral Therapy Management
- Opportunistic Infections Prophylaxis (PCP, MAC)
- Gynecologic Care (pelvic exam with PAP smear, GC culture, Chlamydia screening)
- Tuberculosis Screening

- Substance Use Screening
- Specialty Referrals (dental, ophthalmology)
- Treatment Adherence
- Patient Education
- Access to Expert HIV Care

Indicators specific to Title IV programs include:

- HIV Counseling & Testing for Pregnant Women
- Perinatal Transmission Prophylaxis
- Pediatric Early Diagnosis & PCP Prophylaxis
- Pediatric Antiretroviral Therapy
- Pediatric Neurodevelopmental Exams
- Pediatric Dental Exams

Additional indicators shall be maintained and added through the customization features of ARIES (R37).

6.1.7 SERVICE CONTRACTS

The Financial components of ARIES deal with managing service records and permitting users with the appropriate security roles to allocate services to various contracts and programs defined for the agency. The Financial system starts with configuring the funding sources and contracts for the agency. ARIES shall track federal, state, city and private funding sources (R33, R34, R38, R39). The agency program manager shall have the ability to configure any number of contracts pertinent for the operations of the agency. Each contract shall have a start and end date, a contract total amount, a funding source, and descriptive fields such as contract name and number.

Besides configuring the contracts, the program manager shall have the ability to define the types of services and subservices provided by the agency. The system shall display the Partner-defined service hierarchy and the program manager shall check the types of services provided by an agency. The system shall allow the agency program managers to define agency categories under each appropriate partner subservice. For each agency category, the system shall maintain information regarding the agency category's name, unit of measurement, the default unit and price of service and the one or contract associated with the category.

Once the configuration of the contracts and service categories is complete, users may start to enter service line items (SLI). A service line item is the basic unit of contracts billing and shall be created by users whenever they provide services to a client. Each SLI shall contain information regarding:

- The date of service
- The site where the service was performed
- Name or Staff ID of the person performing the service
- The program for the service
- The service category (limited by the program selection)
- The subservice category (limited by the service selection)
- The agency category (limited by the subservice selection)
- The unit of service, which includes the quantity and rate/unit of service (limited by the agency category selection). The cost of service shall be calculated by quantity multiplied by rate/unit.
- The time spent providing the service
- Notes regarding the service, if any

The system shall provide several features to facilitate rapid data entry, such as the ability to duplicate a SLI record for each date between the service date and the service end date, and the ability to rapidly enter similar service line items one after another.

When the user saves the SLI record, the system shall execute a test to determine if the service record was coded to contracts where there are funds remaining to pay for the service. In configuring the agency services, the program administrator specifies one funding source for the service category. If the new service record amount exceeded the limit, the user shall get a warning notifying him/her that the budget limit had been reached (R40). The user shall then either make changes to the service record or ignore the message.

6.1.8 PROGRAMS

ARIES shall provide two screens for enrollment into, and disenrollment from, programs such as CARE-HIPP, CMP, EIP, MCWP, and TMP. Each of these programs shall also have one or more program-specific screens to collect additional data for that program.

6.2 Administrative Functions

The ARIES system, being designed for several distinct installations, shall have features that shall allow the system administrators to configure and customize the system as appropriate for the installation. Also, because the medical and psychosocial records in

ARIES demand a high level of confidentiality and security, the system shall provide system administrators with the ability to manage different classes of users simply and consistently, so that each group of user shall be able to view data that is appropriate to their role.

6.2.1 Adding and Maintaining Users and Agencies

At each partner installation, the Super-System Administrator (SA) shall have the ability to configure the system and maintain all user accounts, including the ability to create and disable accounts (R41, R72). The system shall be designed to allow additional classes of system administrators who shall be delegated a subset of the privileges of the Super-SA, such as the ability to maintain user accounts and permissions for a specific provider. At no time shall an SA be able to grant rights and privileges to another account that the SA account itself does not possess (R78).

Before a user can be created, the Super-SA shall be required to create the provider and provider sites with which the user is associated (R42). The provider information stored by the system shall include:

- Agency Name
- Contact Info for Representative: email, phone, fax, notes
- Web Site
- Federal Tax ID Number
- Type of provider and ownership status
- Demographic information about the provider’s client, staff and directors
- Information about Sites: site name, address, county, telephone, fax, Health Service Delivery Area (HSDA) Number

To access ARIES, a user shall be required to have a valid account set up by a system administrator. The account shall contain the following information about the user:

- User Name
- Login Name
- Password
- Agency
- Primary site
- Title
- Telephone number
- Email Address

- A set of permissions that the user has, as discussed in the next section.

Each user shall be able to update some of the account information themselves, such as telephone and email address, as well as the password (R41). The user additionally shall be able to choose his/she home page in ARIES.

The Super-SA account shall have the ability to set password policies for each installation (R41). The first policy regards how long a period of inactivity can be before the user is forced to reauthenticate. The second one sets the minimum length of the password and a regular expression for the contents of the password. The system shall automatically reject null passwords. The third policy is the length of time a user shall keep a password before they are forced to change it.

6.2.2 Setting Privileges

Subject to slight refinement, the ARIES system shall have the following groups of functionality and privileges (R43, R73):

- View, create, change or remove Appointments
- View, create, change or remove Client URN Elements
- View, create, change or remove Eligibility Documents
- View, create, change or remove Share Status
- View, create, change or remove Enrollment Date
- View, create, change or remove Client Contact Info
- View, create, change or remove Related/Affected Individuals
- View, create, change or remove Contact by mail, phone, confidential
- View, create, change or remove Client Basic Demographics
- View, create, change or remove Financial
- View, create, change or remove Health Insurance
- View, create, change or remove HIV Classification, AIDS Diagnosis, Karnofsky/CFA
- View, create, change or remove Basic Medical
- View, create, change or remove CD4 and Viral Load
- View, create, change or remove STI
- View, create, change or remove Immunization
- View, create, change or remove Pregnancy

- View, create, change or remove Medications
- View, create, change or remove Risk Factors
- View, create, change or remove Substance Abuse
- View, create, change or remove Mental Health
- View, create, change or remove Legal
- View, create, change or remove Service
- View, create, change or remove Needs Assessment
- View, create, change or remove Care Plan
- View, create, change or remove Referral
- View, create, change or remove Referral Outcome
- View, create, change or remove Legal Notes
- View, create, change or remove Mental Health Notes
- View, create, change or remove Substance Abuse Notes
- View, create, change or remove All Other Notes
- View, create, change or remove Program Enrollment
- View, create, change or remove EIP
- View, create, change or remove Financial Reports
- View, create, change or remove Management Reports
- View, create, change or remove other Reports
- View, create, change or remove Staff
- View, create, change or remove Staff Permissions
- View, create, change or remove Agency
- View, create, change or remove Agency Contracts and Services

After a user account is set up, the system administrator shall be presented with a screen displaying the various security roles to which the user could be assigned. By selecting a role, a grid containing the groups of functionality and privileges above shall be populated with the default privileges for the role. The system administrator shall then be able to add or remove privileges as desired for that particular user. At no point shall the system administrator be able to assign privileges to another user that he/she does not possess.

Using the privileges matrix established by the system administrator, the ARIES system shall determine whether the user would see a link to a specific functionality (if he/she has view privileges); if he/she is in a screen, the system shall determine whether the “New” and “Edit” buttons would be displayed (if he/she has create or edit privileges).

ARIESAdmin will contain screens to create and manage groups using the same grid of permissions. When making a change to a group permission, the administrator will have the option of propagating the change to all the users in that group (after getting a warning that this will overwrite their permission customizations).

6.2.3 MONITORING AND CONTROLLING

The ARIES application shall have a console from which the Super System Administrator can monitor and control certain aspects of the system (R46). The Super-SA can view the versions of all the tools and components of the system such as the database, .NET installation and database driver. To manage access to the system, the console shall allow the Super-SA to see which users are currently connected to the system. The Super-SA shall be able to log out any connected user, who would be informed of that the next time the user attempted to connect to the web server. When doing system maintenance, the Super-SA shall be able to lock all users from the entering the system by using the console.

6.2.4 ERROR LOGGING

To help troubleshoot system errors, the ARIES system shall log all system errors (R5). User errors, such as leaving a required field blank or entering a character in a telephone number field shall be caught and managed in the browser. The system errors captured in this log might be caused by a lost database connection, or an unanticipated syntax error in a generated SQL command, for example. The Super System Administrator shall choose whether the error log shall be maintained in a delimited text file or the Windows event log (R48). The error log shall contain the following information:

- User ID (where available)
- Timestamp
- Client ID (where available)
- Code page
- Exception Code
- Exception Message
- All details of the error including the stack trace.

6.2.5 IMPORT AND EXPORT FUNCTION

The ARIES system shall have facilities to allow users with the appropriate credentials to import and export data to/from the database server. The ARIESImport and ARIESReportExport applications use more restrictive client certificates to limit access. As with the ARIES client management application, all import and export functions shall exchange data over the Internet encrypted via SSL.

Import

There are two contexts for importing data. One involves transferring data from one ARIES installation to another, while the other is getting information into a singular installation, as in the event of data conversion to bring on a new ARIES agency, or importing data from a non-ARIES provider.

In the context of cross-installation data import, the system shall have replication facilities (R54) to permit San Bernardino and San Diego to transmit their Title II, EIP and CMP data to the State of California. Replication shall be implemented either with the built-in SQL Server capabilities, or by using the import function detailed below. The details of what data to replicate shall be determined during system and database design.

The second data import function shall involve submitting data to ARIES in XML format (R53). It shall be done either interactively using a form in ARIESImport, or as a scheduled event using a web service. Before making any change to the database, the Web service shall authenticate the user's access to the service (R56) and validate with XML schema to make sure that the user imported a file that is properly formatted. Then, the system shall validate the values of the fields and records, testing for consistency to business rules such as assigning a service line item to a valid contract. Data for new clients shall be imported in its entirety. For existing clients only the service data will be imported—changes to the client demographics will be ignored. Once the validations have passed successfully, the system shall then invoke the appropriate functions to insert the data into the database. If there are errors in the data, then the entire import will fail. The system shall produce a comprehensive error report that shall allow the import user to understand and correct the errors (R5).

The system shall maintain a log of all imports with information including time, number of records in the import file, number of records imported, error summary, source of the data, mode (interactive or scheduled), and user ID for interactive imports.

Export

The export function of ARIES shall permit users with the proper credentials to extract data from the database (R56). The database server shall decrypt encrypted fields, if the user has the appropriate permission (R52).

The export capability is accessible in two different ways: either a bulk export of all the data for one agency or a fine-grained export of data resulting from a report. Both these capabilities are accessible from the ARIESReport/Export application.

For the bulk export for one agency there shall be a filter on the service date. To do the export the user shall indicate what type of output the system must generate: tab-delimited, comma-separated, or XML (R50). The XML format may be imported directly in Access XP/2002 (R51). The export function will extract the required data and store it on a file of the appropriate format on the server for a limited amount of time. The user shall be presented with a link to the file and can opt to save the file to disk with a right-click over the link and selecting the “Save Target As…” command in the pop-up menu, or to view the file by clicking on the link. The system shall be developed to control access to the download files so that only the user who created a file can access it (R66). The export file shall be encrypted by SSL (R55), as is the entire ARIES communication, when it is transferred from the web server to the client browser.

The second approach to exporting finer-grained parts of the data is tied to the reporting. After generating a report and seeing the results, the user may choose the export button for that specific data. Then they choose the export format and download the file as described above.

6.3 Reporting Function

The ARIES reporting functions allow users within agencies quick access to their data. The ARIES application will contain links to predefined reports through menu items for client, service, management, and financial reports. It will also contain a cross-tab wizard like the one in CareWare.

The ARIESReportExport application will contain a more advanced ad-hoc reporting tool based on views (R90). The most advanced users will use the ARIES export capabilities and use a commercial tool like Crystal, SAS, SPSS, or Access. Users at the Partners shall have access to the full database through ODBC or OLEDB. Encrypted fields shall automatically be decrypted for users with appropriate access (R59).

6.3.1 Report Output

Reports will be produced in HTML. Any column displaying a primary entity, such as client or staff, shall have a hyperlink to support drill-down to the details for that entity. At the bottom of the report shall be a total of the number of rows returned, the date and time the report was generated, and the filter criteria applied.

Each report request screen shall also display a check box labeled "Display print format". When this is checked the report output shall not contain any hyper links or any navigation (buttons or menu bar). The user shall choose to print the report directly with the File->Print menu item in Internet Explorer. The user can use the File->Page Setup menu item in the browser to set the paper size, page orientation, headers and footers, and margins of the printed page.

For more control over the fonts, page breaks, headers, footers, or other formatting, the user shall save the report with the File->Save As menu item (R58). The saved file can be opened or imported into a word processing or spreadsheet program for detailed formatting.

6.3.2 Predefined Reports

The ARIES system shall have a set of predefined reports that give users quick access to frequently used information (R57). When the user selects a report, he/she shall be prompted to filter the report output by entering a date range, program, contract, and so forth. Each report shall have a corresponding set of filter parameters for the user to complete.

When the user clicks the button the server shall generate an HTML page displaying the results of the report request. To use the report in Excel or Access, the user can save the HTML page and then import the data in to Excel or Access with the Get External Data features of these applications (R58). All reports shall run upon the request of the user. Users who would like to be reminded to run certain reports can opt to have a reports page be their home page.

The system shall contain the following predefined reports:

- Missing HRSA Data
- Financial
- Pending Eligibility Documents
- Client Status
- Active Client Roster by Staff
- Referral
- Needs Assessment
- Immunizations
- Staff User
- Disease Management
- Mailing Labels
- Care Plan with Incomplete Tasks
- Unsigned Case Notes

6.3.3 Ad-hoc Reports

Additionally, in ARIESReportExport there shall be a series of screens to support ad-hoc reports via a wizard (R57). The screens will ask which tables to use, how to join them, which columns to display, how to sort them, and how to filter the rows. The results of the choices may be stored as a new quick report on one of the ARIES screens.

The system shall also provide a Cross Tab report that permits the user to choose the fields to display in the rows, the columns, and the strata. An example of a Cross Tab report is to display all zip codes in the rows and counts by HIV disease stage in the columns.

6.3.4 Compliance Reports

The system shall contain the following predefined compliance reports (R60):

- Care Act Data Report
- EIP (California version)
- EIP (Texas version)
- HOPWA
- Case Management Program (California version)
- Case Management Program (Texas version)
- AIDS Waiver
- CARE/HIPP
- Care Services Report (California)
- Programmatic Report (Texas)
- WICY

7 Additional Features

7.1 Options Not Included in Release 1.0

In meetings with the Partners many good ideas were presented for enhancing ARIES. It is not possible to incorporate all these features in the first release, given the time and budget constraints. They are recorded here for consideration in future releases.

- ♦ Scanning eligibility documents into ARIES and incorporating a document management system
- ♦ Printing scanner-friendly data entry forms, scanning the completed forms, and incorporating optical character recognition (OCR) to reduce data entry.

- Supporting deferred updates or store and forward capabilities for home visits.
- Implementing separate applications for different programs (CMP, EIP, etc.)
- Implementing user interfaces that match the current data input forms for CMP, EIP, TMP, etc.
- Assigning staff to programs and limiting visibility of screens based on staff assignment
- Customization of fields or pull-down list box entries at the agency, rather than Partner, level.
- Server-side mail merge or server-side templates for formatted output
- The system shall produce HTML reports in the initial release. Other formats, such as Excel or PDF, can be incorporated into the functionality of future releases.
- Implementing a SQL parser or allowing users to type SQL directly into ARIES
- Tracking expenses such as staff salary and benefits for reimbursement contracts
- Tracking construction, ownership, or leasing costs for buildings under HOPWA

7.2 Correspondence with the Request for Proposals

The references like (R12) in the above text provide links to the requirement numbers in the Request for Proposals (RFP). In the discussions with the Partners, a few requirements were no longer needed, including

- Defining additional objective standard indicators of client progress (R29), rather than using existing data elements such as CD4, Viral Load, Acuity Tool, etc.
- Running reports automatically on user log-in, rather than on demand (R45)
- Record ownership (R75, R76): The Partners decided that they did not want this feature because it would hinder the ability to share a client’s record across multiple agencies.